IN THE SPECIFICATION

Please amend the specification to insert the following four paragraphs (reflecting the allowed claims) in the Summary of the Invention section, at the end of page 4 and prior to the Brief Description of the Drawings section on page 5.

In another aspect, a method of securely delivering data is provided. The method includes creating a container having electronic content and a container identifier, encrypting at least one data block of the electronic content using a symmetric encryption technique and encrypting a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key, and re-keying the header using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device, wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier.

In another aspect, a computer program product comprising a computer usable medium having readable program code embodied in the medium is provided. The computer program product includes at least one component to create a container having electronic content and a container identifier, determine at least one data block for partitioning the electronic content, encrypt the at least one data block of the electronic content using a symmetric encryption technique

and to encrypt a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key, re-key the header using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device, wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier, and decrypt the locked portion of the electronic content when the user or user's device has been authenticated.

In another aspect, a computer-implemented method of securely delivering data is provided. The computer-implemented method includes creating a container having electronic content and a container identifier, encrypting at least one data block of the electronic content using a symmetric encryption technique and encrypting a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key, and re-keying the header using at least a portion of the container identifier and data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device, wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier, and wherein the step for re-keying creates a unique value for the header for every different container delivered to the user's device.

In another aspect, a computer-based method for accessing content is provided. The method includes transmitting an electronic container having files of electronic content and a container identifier, wherein at least one data block of the electronic content is encrypted using a symmetric encryption technique and a header associated with a first data block of the electronic content is encrypted using an asymmetric encryption technique, the header including a symmetric decryption key, and transmitting a permission token based on an attempt to access the electronic content to grant access to the electronic content, wherein at least the symmetric decryption key is re-encrypted for each occurrence of transmitting the permission.

Please amend the paragraph starting at page 1, line 14, with the following:

Any owner or distributor of secure or copyrighted digital content, i.e., electronic data in any form, may face several problems concerning the encryption of the data and the method of access that is provided to an end user. The owner or distributor typically is compelled to provide a robust method of encryption while remaining within a system that is relatively easy and simple for users to operate. In order to be relatively effective and/or easy to use, the system provided by owners or distributors must typically allow users to repeatedly access the material while requiring that they undergo an authentication, approval or payment process under a set of rules determined by the content owner. For example, the user may access the content an unlimited number of times after approval, or the user may have to regain approval after a certain number of

accesses and/or [[a]] after a certain amount of time has passed. Normally, content owners require substantial confidence and assurance that once approved for access by a particular user on a particular device the content cannot be freely accessed by another user especially if the content is transmitted to another machine or device.

Please amend the paragraph starting at page 3 line 18, with the following:

A further aspect of the invention includes a system for creating a digital container and encrypting the contents of the digital container with a symmetric encryption technique. The system also provides for protecting the ~~systemic~~ symmetric decryption keys by inserting the symmetric decryption keys into header associated with a data block in the digital container and encrypting the header using an asymmetric encryption algorithm. Upon an attempted access of the container by a user, the system re-encrypts the header using data from the user's device such as a machine footprint and/or the user such as a client fingerprint so that the contents of the digital container are now locked to the user's device or to the user. The system may also acquire transaction data such as credit card information or account information from the user, perhaps for paying for the contents of the container or other service, which may be verified and used to gain access to the contents. Once the container has been locked to the user's device or user, the system provides that the container may only be opened and accessed on that device or by that user. If the digital container were to be transmitted to another device, the system recognizes that the footprint of the

device has changed or the user is different and may not open until a re-authorization has been performed which may involve a financial transaction.

Please amend the paragraph starting at page 6 line 7, with the following:

An aspect of the invention involves a unique process that is used to "re-key" the "hidden" keys sent with the electronic content, often in digital containers, with a value that contains data specific to the user and/or the user's device. This "re-keying" (i.e., re-encrypting) is typically performed on the user's device without ever exposing the content in an unencrypted form, thus the keys themselves are maintained securely and eliminates the potential for compromising the electronic data and/or the keys. During "re-keying", the "re-keyed" keys may also be associated with the original user's device in such a way as to effectively inhibit any unauthorized ~~assess~~ access to the electronic content. This is especially useful, if and when, the electronic content might be further propagated to other user's devices, such as by email, copied disks, or peer-to-peer communications, for example. These other users are effectively denied access to the electronic content since the electronic content has been re-keyed and associated with the original user and/or original user's device. After the "re-keying" process executes, the content inside the container is "locked" to a particular device and/or a particular user.

Please amend the paragraph starting at page 8 line 1, with the following:

The system 100 may also include a container authentication server 160 (also referred to as a container verification server), which in embodiments, may oversee operations of a container registration database 165. In embodiments, database 165 may be distributed. The container authentication server also manages attempts to open the container by a user and coordinates permissions, authentications and portions of the re-keying sequences of a digital container using the container ID and container registration database 165. This may also include managing financial transactions associated with the container ~~assess~~ access. Also included in the system 100 may be a transaction server 180 (e.g., an IPayment, Inc. Gateway server) for receiving financial transaction requests such as credit card or debit transactions when a user chooses to purchase a service or item controlled by the SDC 120', and for providing a response to the request which validates a purchase, as described more fully below.

Please amend the paragraph starting at page 8 line 13, with the following:

In one application, the container creation application 110 encrypts the one or more content files ~~105~~ 115 (or any subset of the content files) and incorporates the one or more content files ~~105~~ 115 into the secure digital container 120. Once the SDC 120 has been constructed, usage rights parameters as selected by the content originator, along with other SDC registration data, may be stored in the container registration database 165, as denoted by reference numeral 170. The usage rights may include, but not limited to, limiting accesses

to the content files to a certain number of occurrences, limiting access to a period of time, limiting copying of the content files (or portions thereof), limiting the copying to a secondary device, limiting the burning of the content file to storage media such as CD or DVD or controlling printing, to name a few.

Please amend the paragraph starting at page 11 line 1, with the following:

Figure 2 is a functional block diagram of an embodiment showing registration and encryption of a SDC, according to the invention, generally denoted by reference numeral 200. Figure 2 also illustrates certain steps of the registration and encryption process, according to the invention. The container creation application ~~105~~ 110 evaluates the content file(s) 115 as selected or composed by a container creator and determines an appropriate number of data blocks for partitioning the content files and to be used to encrypt these files. The number of data blocks to be encrypted may be related to the type of device being targeted (e.g., a cable box, personal computer, or other type of device), number of files being encrypted, or overall amount of data being encrypted, or as requested by a container creator, for example. The data block concept typically increases speed and efficiency of the decryption process. Also, the data block concept provides an ability to encrypt only parts of the electronic content instead of the entirety and also permits portions of the content to be optionally accessed by a user prior to any decryption. For example, if a large media file, such as a feature length motion picture is being decrypted, the user may be able to use a media player to jump to any point in the film and begin to view it without

waiting for the entire file to be decrypted. Another example may be when advertisement segments, such as previews, are presented to a user prior to decryption. It should be clear by these examples that essentially any portion of the electronic material may be selected by the container creator and marked as "unencrypted," as appropriate.

Please amend the paragraph starting at page 11 line 21, with the following:

Once the content file or files 115 are divided into data blocks, a symmetric encryption algorithm 112 may be used to encrypt each individual data block resulting in one or more encrypted data blocks 1-N, 230a – 230c. The encryption process and insertion into the SDC 120 for each encrypted data block 230a-230c is represented by reference numerals 245a-245c, respectively. Commercially available symmetric encryption algorithms such as, for example, Blowfish™, Twofish™, Rijndael™, Serpent™ or Triple DES™ may be used. The container creation application ~~105~~ 110 may be designed in a modular fashion, so that the encryption algorithm modules can be upgraded as new encryption technology becomes available.

Please amend the paragraph starting at page 12 line 15, with the following:

The asymmetric encryption algorithm 205 generates two decryption keys, called the primary and secondary keys 250 and 252, respectively, and are stored in a record 225 in the container registration database 165 on the container verification server 160. The primary 250 and secondary key 252 are associated

with the corresponding unique SDC 120 via digital container ID 210 (also referred to as unique container ID) (e.g., 12345). Reference numeral 220 denotes the logical association of the digital container ID 210, the primary key 250 and the secondary key 252 for each unique record in the container registration database 165.

Please amend the paragraph starting at page 19 line 1, with the following:

These usage rights parameters may be encrypted by a symmetric encryption algorithm 575. The previously created fingerprint key 565 may be used as the encryption key for this process. The resulting encrypted usage rules 585 data may then be provided to the token assembler 590. The previously created atomic proxy re-key value 580 may also be sent to the token assembler 590 along with a permission flag data string 594 (also known as an installation flag) and any encrypted financial transaction response 194 data 596, previously created by the transaction server 180.

Please amend the paragraph starting at page 20 line 1, with the following:

Figure 6 is an illustration of an embodiment of a permission token, according to the invention, generally denoted by reference numeral 600. The exemplary permission token 600 includes fields for a header 605 to indicate the beginning of the token, an installation permission flag 610, an atomic proxy re-key value 615, a client fingerprint mode flag 620, digital rights management usage rules data 625, a financial transaction response data 630, and a trailer 635

to indicate the end of the token. These fields of the permission token 600 are built by the token assembler 590, previously described, for transmission in a message to the SDC on the user's device. The use of these fields at the user's device is described in relation to Figure 7.

Please amend the paragraph starting at page 21 line 1, with the following:

The executable instructions employ a machine footprint ~~algorithm~~ module 720 that uses the CFMF 330 value to determine what subset 722 of the original machine footprint sources 725 is used to create the machine footprint subset 720 that matches the similar subset created on the container authentication server 160 during the token assembly process. Once the machine footprint subset 722 is determined, it is used by the machine footprint module 720 to create the fingerprint key 730.

Please amend the paragraph starting at page 21 line 7, with the following:

The fingerprint key 730 is used by an asymmetric ~~encryption~~ decryption algorithm 735 to decrypt the re-encrypted header of the first content data block 231. Once the header decryption process is completed, the fingerprint key 730 may be discarded and therefore no decryption key is stored on the user's machine and available for hacking or reverse engineering. Throughout this process, the container and its content(s) are securely locked to the user's machine 125. Since the fingerprint key 730 is not stored on the user's device 125, it is re-created every time the user attempts to open the container.